CLAIMS

What is claimed is:

1. A method of establishing a consistent password policy, said method comprising:

describing a plurality of password policies in a computer usable password policy data structure;

accessing said computer usable password policy data structure by a password policy enforcement agent; and

enforcing at least one of said plurality of password policies described within said password policy data structure by said password policy enforcement agent.

2. The method of Claim 1 wherein said computer usable password policy data structure comprises a file structure substantially compatible with extensible markup language.

3. The method of Claim 1 wherein said password policy enforcement agent is operable on a client computer of a client-server computer system.

4. The method of Claim 1 operable on a utility data center.

5. The method of Claim 1 further comprising validating said computer usable password policy data structure for authenticity by said password policy enforcement agent.

6. The method of Claim 1 wherein said plurality of password policies comprises a threshold parameter for unsuccessful access attempts that when exceeded disables a computer system access account.

7. The method of Claim 6 wherein said plurality of password policies comprises a parameter indicating the a time duration within which said threshold parameter number of unsuccessful access attempts triggers locking of a computer system access account.

8. The method of Claim 1 wherein said plurality of password policies comprises an initial delay parameter to block access to a computer system access account for a period of time after an unsuccessful access attempt.

9. The method of Claim 8 wherein access to said computer system access account is delay for an increasing time period for successive unsuccessful access attempts.

10. The method of Claim 1 wherein said plurality of password policies comprises a minimum password length parameter.

11. The method of Claim 1 wherein said plurality of password policies comprises a maximum password length parameter.

12. The method of Claim 1 wherein said plurality of password policies comprises parameter to prohibit passwords consisting of a natural language word.

13. The method of Claim 1 wherein said natural language is English.

14. The method of Claim 1 wherein said plurality of password policies comprises parameter to prohibit passwords consisting of a palindrome.

15. The method of Claim 1 wherein said plurality of password policies comprises parameter to prohibit passwords consisting of a derivative of a computer system account name.

16. The method of Claim 1 wherein said plurality of password policies comprises parameter to automatically generate a password.

17. The method of Claim 16 wherein said plurality of password policies comprises parameter to automatically generate a pronounceable password consistent with all of said plurality of password policies.

18. The method of Claim 16 wherein said plurality of password policies comprises parameter to specify a set of characters utilizable to automatically generate a password.

19. The method of Claim 1 further comprising providing, by said password policy enforcement agent, feedback to a configuration and aggregation point, about which of said plurality of password policies have been successfully enforced.

20. A computer usable password policy data structure comprising computer access password policy parameters.

21. The computer usable password policy data structure of Claim 20 comprising a file structure substantially compatible with extensible markup language.

22. The computer usable password policy data structure of Claim 20 comprising a computer access password policy parameter selected from the set of computer access password policy parameters comprising:

a threshold parameter for unsuccessful access attempts that when exceeded disables a computer system access account;

a parameter indicating the a time duration within which said threshold parameter number of unsuccessful access attempts triggers locking of a computer system access account;

an initial delay parameter to block access to a computer system access account for a period of time after an unsuccessful access attempt;

a minimum password length parameter;

a maximum password length parameter;

a parameter to prohibit passwords consisting of a natural language word;

a parameter to prohibit passwords consisting of a palindrome;

a parameter to prohibit passwords consisting of a derivative of a computer system account name;

a parameter to automatically generate a password;

a parameter to automatically generate a pronounceable password consistent with all of said plurality of password policies; and

a parameter to specify a set of characters utilizable to automatically generate a password.

23. A computer system comprising:

a first server computer for controlling access to said computer system;

a second server computer coupled to said first server computer for providing control of said computer system;

computer usable media comprising computer usable instructions than when executed on a processor of said first server computer implement a method of establishing a consistent password policy, said method comprising:

accessing a computer usable password policy data structure; and

enforcing a password policy described within said password policy data structure.

24. The computer system of Claim 23 comprising a utility data center.